CLAIMS

1. A method of executing code of at least one software program in a multi-processor computer environment, each software program including (i) a first portion of software code to be executed in a computer, and (ii) a second portion of software code that includes one or more fragments of code of the software program, the method comprising executing the second portion of code in one or more external devices which are in communication with the computer.

2. The method of claim 1 wherein the second portion of code is encrypted, the method further comprising transferring the second portion of code to a secure computer environment, and decrypting the second portion of code in the one or more external devices prior to execution.

3. The method of claim 2 wherein the one or more external devices are one or more smart cards, each smart card including a processor for executing the second portion of code, the smart card being the secure computer environment.

4. The method of claim 1 wherein the fragments of code are interspersed within the first portion of code.

5. The method of claim 1 wherein the second portion of code is stored in the computer, the method further comprising downloading the second portion of code into the one or more external devices prior to execution.

6. The method of claim 1 wherein there are a plurality of software programs, and the second portions include fragments from more than one of the software programs.

7. The method of claim 1 wherein the one or more external devices are tamper-resistant.

8. The method of claim 1 wherein the one or more external devices are one or more smart cards.

9. An apparatus which executes code of at least one software program in a multi-processor computer environment, each software program including (i) a first portion of software code, and

(ii) a second portion of software code that includes one or more fragments of code of the software program, the apparatus comprising:
(a) a first computer which executes the first portion; and
(b) one or more externals unit in communication with the computer, the one or more external units executing the second portion.

10. The apparatus of claim 9 wherein the second portion of code is encrypted, the apparatus further comprising:
(c) means for transferring the second portion of code to a secure computer environment; and
(d) means for decrypting the second portion of code in the one or more external devices prior to execution.

11. The apparatus of claim 10 wherein the one or more external devices are one or more smart cards, each smart card including a processor for executing the second portion of code, the smart card being the secure computer environment.

12. The apparatus of claim 9 wherein the second portion of code is stored in the computer, the apparatus further comprising:
(e) means for downloading the second portion of code into the one or more external devices prior to execution.

13. The apparatus of claim 9 wherein the one or more external devices are tamper-resistant.

14. The apparatus of claim 9 wherein the one or more external devices are one or more smart cards.

15. A method of transforming a computer program which includes software code, the method comprising:
(a) identifying one or more fragments of the software code,
(b) associating a program call with each of the identified fragments; and
(c) inserting the program call into the software code, thereby transforming the software program,

wherein when a program call is reached, the respective fragment of software code is executed.

16. The method of claim 15 further comprising:
(d) encrypting the software code associated with the identified fragments; and
(e) replacing the fragments with encrypted versions of the software code.

17. A method of executing a computer program which includes software code, the software code having (i) a first portion, and (ii) a second portion, the second portion including one or more fragments of the software code and a program call associated with each fragment, the method comprising:
(a) executing the first portion; and
(b) executing the associated fragments when a program call in the second portion is reached.

18. The method of claim 17 wherein the first portion executes in a computer, and the second portion executes in an external device with respect to the computer, and step (b) further comprises sending a fragment to the external device when a program call of the associated fragment is reached, and executing the fragment in the external device.

19. The method of claim 18 wherein step (b) further comprises generating a result upon execution of the fragment in the external device, the result being used during subsequent execution of the computer program.

20. The method of claim 18 wherein the external device is a smart card.

21. The method of claim 17 wherein the one or more fragments are encrypted code, the method further comprising:
(c) decrypting the one or more fragments prior to execution thereof.

22. An apparatus for executing a computer program which includes software code, the software code having (i) a first portion, and (ii) a second portion, the second portion including one or more fragments of the software code and a program call associated with each fragment, the

apparatus comprising:

(a) means for executing the first portion; and

(b) means for executing the associated fragments when a program call in the second portion is reached.

23. The apparatus of claim 22 wherein the means for executing the first portion is in a computer, and the means for executing the associated fragments is in an external device with respect to the computer, and a fragment is sent to the external device when a program call of the associated fragment is reached, and is then executed in the external device.

24. The apparatus of claim 23 wherein the external device is a smart card.

25. The apparatus of claim 22 wherein the one or more fragments are encrypted code, the apparatus further comprising:

(c) means for decrypting the one or more fragments prior to execution thereof.

26. A method of access control of software code which is executed on a smart card that is in communication with a host computer, the smart card having stored therein access control parameters for identified software code, the method comprising:

(a) the host computer uploading software code and its identity data to the smart card; and

(b) the smart card using the access control parameters and the identity data to determine whether access is permissible for the uploaded software code, wherein the software may be executed only if access is permissible.

27. The method of claim 26 wherein the software code includes one or more fragments of software code of a software program that executes at the host computer.

28. The method of claim 26 wherein access control parameters include one or more of permission status, number of runs data, time data, and program variant data.

29. The method of claim 26 further comprising:

(c) modifying at least one of the access control parameters subsequent to an initial storage of the access control parameters.

30. A method of executing a plurality of software code fragments of a software program on an external unit, wherein the external unit is connected to a computer, the external unit including a processor and a memory, the method comprising:
(a) at execution time of each of the software code fragments, automatically uploading the respective software code fragment to the memory of the external unit; and
(b) executing the respective software code fragment in the external unit using only the processor and the memory of the external unit.

31. The method of claim 30 wherein the software code fragments are encrypted, the method further comprising:
(c) after step (a) and prior to step (b), decrypting the software code fragments.

32. A method of preparing code of a software program, the software program including (i) a first portion of source code to be executed by a first processor, and (ii) a second portion of source code to be executed by a second processor, the second portion of source code including one or more fragments of code of the software program, the method comprising prior to compilation of the software program, encrypting only the second portion of source code.

33. The method of claim 32 wherein the second processor is a smart card.